

**BLAKELY SOKOLOFF TAYLOR & ZAFMAN**

A LIMITED LIABILITY PARTNERSHIP INCLUDING LAW CORPORATIONS

TELEPHONE (408) 720-8300

FACSIMILE (408) 720-8383

BSTZ\_MAIL@BSTZ.COM

WWW.BSTZ.COM

INTELLECTUAL PROPERTY LAW

SILICON VALLEY

1279 OAKMEAD PARKWAY  
SUNNYVALE, CALIFORNIA 94085-4040

OTHER OFFICES

LOS ANGELES, CA  
ORANGE COUNTY/COSTA MESA, CA  
SAN JOSE, CA  
DENVER, CO  
PORTLAND/BEAVERTON, OR  
SEATTLE, WA**FACSIMILE TRANSMITTAL SHEET**DELIVER TO: Examiner Truong CamquyFACSIMILE NO.: (571) 273-3773 TELEPHONE NO.: (571) 272-3773FROM: Michelle Begay for Marina PortnovaDATE: April 18, 2008TOTAL NUMBER OF PAGES INCLUDING COVER SHEET: 10OPERATOR: Michelle Begay OUR REF.: 42P14183

Message:

Examiner Camquy:

Enclosed please find the singed amendment for the above case.

Thank you,

Michelle Begay  
Secretary to Marina Portnova  
(408) 720-8300 x3493IF YOU DO NOT RECEIVE ALL THE PAGES, OR IF THERE IS ANY DIFFICULTY IN RECEIVING, PLEASE  
CALL (408) 720-8300 AND ASK FOR THE OPERATOR NAMED ABOVE.

42P14183

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:	)	
	)	
Gilbert Neiger, et al.	)	Examiner: Truong Camquy
	)	
Application No.: 10/663,206	)	Art Unit: 2195
	)	
Filed: September 15, 2003	)	
	)	
For: Use Of Multiple Virtual Machine	)	
Monitors To Handle Privileged	)	
Events	)	

Mail Stop Amendment  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, VA 22313-1450

AMENDMENT

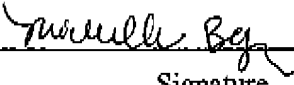
Sir:

Applicants respectfully request the Examiner to enter the following amendments and consider the following remarks:

FACSIMILE TRANSMITTAL

I hereby certify that this correspondence is being transmitted by facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, in accordance with 37 CFR § 1.6(d), on the date shown below.

on April 18, 2008  
 Date of transmission

Michelle Begay  
 Name of Person Faxing Correspondence  
  
 Signature  
 April 18, 2008  
 Date

42P14183

1

**IN THE SPECIFICATION**

**Please replace paragraph [0015] with the following:**

[0015] Thus, a machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer), such as a machine-readable storage medium (e.g., floppy diskettes, optical disks, Compact Disc, Read-Only Memory (CD-ROMs), and magneto-optical disks, Read-Only Memory (ROMs), Random Access Memory (RAM), Erasable Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM), magnetic or optical cards, flash memory), ~~and a machine-readable transmission medium (e.g., a transmission over the Internet, electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.)).~~

**IN THE CLAIMS**

1. (Previously Presented) A method comprising:  
  
detecting an occurrence of one of a plurality of privileged events in a virtual machine (VM) environment having guest software and a plurality of virtual machine monitors (VMMs), wherein the plurality of VMMs is designated to handle the plurality of privileged events that ~~is~~ cannot be handled by the guest software in the VM environment;  
  
determining which one of the plurality of VMMs is to handle the detected privileged event based on at least one of a characteristic of the detected privileged event or characteristics of the VMMs; and  
  
transitioning control to said one of the plurality of VMMs.
2. (Original) The method of claim 1 wherein the plurality of VMMs includes a main VMM and one or more parallel VMMs.
3. (Previously Presented) The method of claim 1 wherein determining which one of a plurality of VMMs is to handle the detected privileged event comprises:  
  
determining a type of the detected privileged event; and  
  
identifying one of the plurality of VMMs that is designated to handle privileged events of the determined type.
4. (Previously Presented) The method of claim 1 wherein determining which one of a plurality of VMMs is to handle the detected privileged event comprises:  
  
accessing a field associated with the detected privileged event in a resource; and

identifying one of the plurality of VMMS that is designated to handle the detected privileged event based on a value of the field.

5. (Previously Presented) The method of claim 4 wherein the field associated with the detected privileged event is a field associated with a type of the detected privileged event.

6. (Previously Presented) The method of claim 4 wherein the field associated with the detected privileged event is a field associated with an input-output address range to which an input-output address of the detected privileged event belongs.

7. (Previously Presented) The method of claim 4 wherein the value of the field associated with the detected privileged event is either predetermined or dynamically configurable.

8. (Previously Presented) The method of claim 1 wherein determining which one of a plurality of VMMS is to handle the detected privileged event comprises:

evaluating resource usage parameters of the plurality of VMMS; and

identifying one of the plurality of VMMS that is designated to handle the detected privileged event based on evaluation of the resource usage parameters.

9. (Original) The method of claim 4 wherein the resource resides in any one of a memory, a processor, a chipset, and an input-output device.

10. (Previously Presented) The method of claim 1 wherein the detected privileged event represents any one of an interrupt, an exception, an execution of a privileged instruction, and a platform event.

11. (Previously Presented) The method of claim 1 wherein the detected privileged event occurs during an operation of guest software.

12. (Previously Presented) The method of claim 1 wherein the detected privileged event occurs during an operation of one of the plurality of VMMs.

13. (Currently Amended) A system comprising:

a memory having stored therein a plurality of virtual machine monitors (VMMs) designated to handle a plurality of privileged events; and

a processor, coupled to the memory, the processor comprising routing logic to detect an occurrence of one of the plurality of privileged events that cannot be handled by guest software, to determine which one of the plurality of VMMs is to handle the detected privileged event based on at least one of a characteristic of the detected privileged event or characteristics of the VMMs, and to transition control to said one of the plurality of VMMs.

14. (Original) The system of claim 13 wherein the plurality of VMMs includes a main VMM and one or more parallel VMMs.

15. (Previously Presented) The system of claim 13 wherein the routing logic is to determine which one of the plurality of VMMs is to handle the detected privileged event by determining a

type of the privileged event, and identifying one of the plurality of VMMs that is designated to handle privileged events of the determined type.

16. (Previously Presented) The system of claim 13 wherein the routing logic is to determine which one of the plurality of VMMs is to handle the detected privileged event by evaluating resource usage parameters of the plurality of VMMs, and identifying one of the plurality of VMMs that is designated to handle the detected privileged event based on evaluation of the resource usage parameters.

17. (Previously Presented) The system of claim 13 wherein the detected privileged event represents any one of an interrupt, an exception, an execution of a privileged instruction, and a platform event.

18. (Previously Presented) The system of claim 13 wherein the detected privileged event occurs during an operation of guest software.

19. (Previously Presented) The system of claim 13 wherein the detected privileged event occurs during an operation of one of the plurality of VMMs.

20. (Previously Presented) A system comprising:

a memory having stored therein guest software and a plurality of virtual machine monitors (VMMs) designated to handle a plurality of privileged events; and

a processor, coupled to the memory, to execute the guest software, to detect an occurrence of one of the plurality of privileged events that cannot be handled by the guest

software, to determine which one of the plurality of VMMs is to handle the detected privileged event based on at least one of a characteristic of the detected privileged event or characteristics of the VMMs, and to transition control to said one of the plurality of VMMs.

21. (Original) The system of claim 20 wherein the plurality of VMMs includes a main VMM and one or more parallel VMMs.

22. (Previously Presented) The system of claim 20 wherein the processor is to determine which one of the plurality of VMMs is to handle the detected privileged event by determining a type of the privileged event, and identifying one of the plurality of VMMs that is designated to handle privileged events of the determined type.

23. (Previously Presented) The system of claim 20 wherein the processor is to determine which one of the plurality of VMMs is to handle the detected privileged event by evaluating resource usage parameters of the plurality of VMMs, and identifying one of the plurality of VMMs that is designated to handle the detected privileged event based on evaluation of the resource usage parameters.

24. (Original) The system of claim 20 wherein the privileged event represents any one of an interrupt, an exception, an execution of a privileged instruction, and a platform event.

25. (Previously Presented) The system of claim 20 wherein the detected privileged event occurs during operation of any one of guest software and one of the plurality of VMMs.



26. (Previously Presented) A machine-readable storage medium storing instructions which, when executed by a processing system, cause the processing system to perform a method, the method comprising:

detecting an occurrence of one of a plurality of privileged events in a virtual machine (VM) environment having guest software and a plurality of virtual machine monitors (VMMs), wherein the plurality of VMMs is designated to handle the plurality of privileged events that cannot be handled by the guest software in the VM environment;

determining which one of the plurality of VMMs is to handle the detected privileged event based on at least one of a characteristic of the detected privileged event or characteristics of the VMMs; and

transitioning control to said one of the plurality of VMMs.

27. (Original) The machine-readable medium of claim 26 wherein the plurality of VMMs includes a main VMM and one or more parallel VMMs.

28. (Previously Presented) The machine-readable medium of claim 26 wherein the detected privileged event represents any one of an interrupt, an exception, an execution of a privileged instruction, and a platform event.

29. (Previously Presented) The machine-readable medium of claim 26 wherein the detected privileged event occurs during operation of any one of guest software and one of the plurality of VMMs.

**REMARKS**

Applicants respectfully request consideration of the subject application as amended herein. This Amendment is submitted in response to the telephone call with the Examiner on April 17, 2008. In this amendment, claim 13 has been amended. No new matter has been added.

**DEPOSIT ACCOUNT AUTHORIZATION**

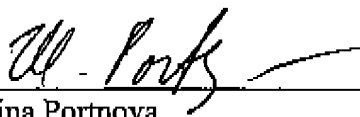
Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Marina Portnova at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: April 18, 2008

  
\_\_\_\_\_  
Marina Portnova  
Reg. No. 45,750

1279 Oakmead Parkway  
Sunnyvale, CA 94085-4040  
(408) 720-8300